Computer Communications 65 (2015) 35–42

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Achieving efficient and privacy-preserving multi-feature search for mobile sensing

Hongwei Li [a,b,*], Yi Yang [a], Haomiao Yang [a], Mi Wen [c]

[a] School of Computer Science and Engineering, University of Electronic Science and Technology of China, China
[b] State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093), China
[c] College of Computer Science and Technology, Shanghai University of Electric Power, Shanghai, China

ARTICLE INFO

Article history:
Available online 21 February 2015

Keywords:
Mobile sensing
Multi-feature
Searchable encryption
Preference weight

ABSTRACT

Currently, more and more mobile terminals embed a number of sensors and generate massive data. Effective utilization to such information can enable people to get more personalized services, and also help service providers to sell their products accurately. As the information may contain privacy information of people, they are typically encrypted before transmitted to the service providers. This, however, significantly limits the usability of data due to the difficulty of searching over the encrypted data. To address the above issues, in this paper, we first leverage the secure kNN technique to propose an efficient and privacy-preserving multi-feature search scheme for mobile sensing. Furthermore, we propose an extended scheme, which can personalize query based on the historical search information and return more accurate result. Using analysis, we prove the security of the proposed scheme on privacy protection of index and trapdoor and unlinkability of trapdoor. Via extensive experiment on real-world cloud systems, we validate the performance of the proposed scheme in terms of functionalities, computation and communication overhead.

1. Introduction

Currently, more and more mobile terminals are equipped with an increasing range of sensing, computational, storage and communication resources [1]. They not only serve as mobile device for computing and communication, but also come with a rich set of embedded sensors [2,3]. More users' activities are monitored, such as walking, driving and sitting. This is approved by people who want to obtain more preferable services. For this goal, users' states should be aggregated and classified to provide accessible service to search entities. The different search entities can filter mobile users and sell the corresponding personalized services [4].

Unfortunately, since the states of users may contain privacy information (e.g., location), malicious use toward it threatens the users' privacy [5], thereby limits the application of sensing information. It is significantly important to find a method to use the information with privacy preservation. Considering the limited capability of the mobile terminals, the method must achieve both privacy preservation and efficiency. Searchable symmetric encryption (SSE) allows confidential search over encrypted data and can achieve more efficiency than other searchable encryption schemes. This method outsources some encrypted indexes and then generates encrypted trapdoor to match. Many SSE schemes in cloud environment have been proposed in order to achieve the same search functionalities as plaintext search. Cao et al. [6] propose a searchable encryption scheme based on secure *k*-nearest neighbor (kNN) computation [7], which supports coordinate matching, i.e., as many matches as possible. And Yu et al. [8] propose a multi-keyword top-k retrieval scheme with fully homomorphic encryption, which can return ranked results and achieve high security.

However, searchable encryption application in mobile sensing has not been studied well. In this paper, we propose an efficient and privacy-preserving multi-feature search scheme for mobile sensing, which can not only achieve secure and efficient multi-feature search, but also return preferable result based on relevance feedback [9–11]. In our scheme, mobile terminals generate some features according to their own states, then encrypt and outsource them to a cloud server. The search entities can also create an encrypted trapdoor to query those encrypted features. Overall, we summarize our original contributions in two aspects as follows:

- We propose an efficient and privacy-preserving multi-feature search scheme for mobile sensing. Security analysis shows that the proposed scheme can achieve privacy protection of index and trapdoor and unlinkability of trapdoor. Extensive

* Corresponding author.
E-mail address: hongweili@uestc.edu.cn (H. Li).

http://dx.doi.org/10.1016/j.comcom.2015.02.006
0140-3664/

experiment results demonstrate the performance of the proposed scheme in terms of functionalities, computation and communication overhead.
- To accurately provide personalized service, we propose an extended scheme by embedding relevance feedback. With the feedback of historical search information, we add preference factor in new query to achieve more precise search.

The remainder of this paper is organized as follows. In Section 2, we outline the system model, security requirements and design goals. In Section 3, we describe the preliminaries of the proposed schemes. We present the developed scheme and extended scheme in Sections 4 and 5, respectively. Then we carry out the security analysis and performance evaluation in Sections 6 and 7, respectively. We provide a review of the related works in Section 8. Finally, we conclude the paper in Section 9.

2. System model, security requirements and design goals

2.1. System model

As shown in Fig. 1, our scheme consists of four entities.

- *Mobile user*: The mobile user represents mobile terminal which may be mobile phone and mobile computer, etc. It can receive mobile services for some corresponding service providers. Some features, represent its own state, can be used to get more personalized services. It outsources its encrypted features to re-encryption agency. To protect feature privacy, the mobile user encrypts the original features through secure encryption algorithm, and generates an index for efficient search. After that, the mobile user sends its identity and the corresponding index to the re-encryption agency.
- *Re-encryption agency*: The re-encryption agency is used to re-encrypt the indexes generated by mobile users and then outsources the re-encrypted indexes to the cloud server. With such an agency, we can avoid key sharing problem of the mobile users. The secret keys of mobile users will not be the same. A mobile user cannot identify the index generated by another mobile user. Besides, the re-encryption agency only has re-encryption keys, thus it cannot get any privacy information from the indexes.
- *Cloud server*: The cloud server is an intermediate entity which stores the identities of mobile users and the encrypted indexes, and then provides access and search services to authenticated search entities. When a search entity sends a trapdoor to the cloud server, it would return a collection of matching identities based on certain operations.
- *Search entity*: An authenticated search entity can be any mobile or fixed entity in the real world. When it wants to search the outsourced information stored in the cloud server. It will generate a search feature set. Then according to the feature set, the search entity uses corresponding secret keys to generate a trapdoor and sends it to the cloud server. Finally, it can receive a result collection of matching identities from the cloud server.

2.2. Security requirements

In this paper, the cloud server is considered as semi-trust, i.e., it may try to attain sensitive information from the queries of search entities while performing the keyword-based search. We define the security requirements as follows:

- *Privacy protection of index and trapdoor*: It is the most basic security feature in general searchable encryption schemes. Without the privacy protection of them, searchable encryption is out of the question. Namely, our scheme should achieve this security requirement.
- *Unlinkability of trapdoor*: We define the unlinkability of trapdoor in a harsh model, **Known Background Model** [12], to study more comprehensive security of our scheme. In this case, the cloud server is more powerful and can possess more statistical information from a known comparable dataset, such as the information of all indexes and trapdoors. Even some keyword information has been leaked, we should achieve that there would not produce any link between any information, and prevent more losses even if a part of the information has been leaked.
- *Access pattern*: Access pattern is the retrieval of sequential searches, consisting of the returned identity sets according to the corresponding search feature sets. Some searchable encryption proposals, e.g., [13], have been proposed to hide the access pattern using private information retrieval (PIR) technique [14]. However, our proposal is not specifically designed to protect the

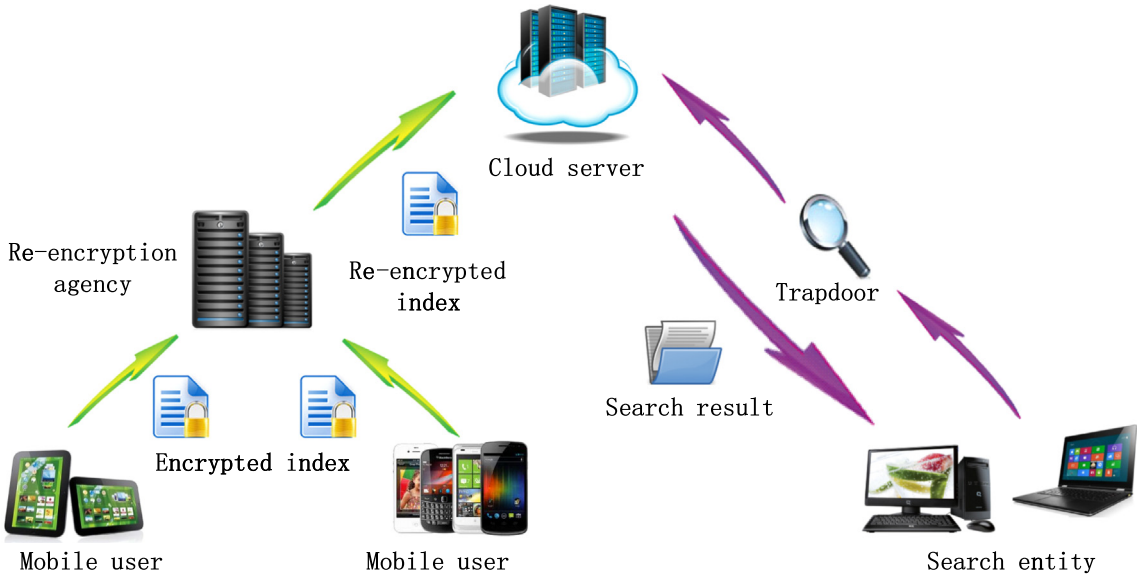

Fig. 1. System model.